IN THE CLAIMS:

Claims 22, 24, and 25 have been cancelled. Claims 30 and 31 have been added. Claims 1 - 21, 23, and 25 - 29 have been amended, as follows:

1. (currently amended) A method, comprising:

~~establishing a physical channel between a sender and a receiver;~~

sending, from [[the]] a sender to [[the]] a receiver, data through a data channel, the data including a key and a nonce;

receiving, at the receiver, the data; [[and]]

establishing a visual physical channel between the sender and the receiver, the sender and receiver being visible to each other; and

verifying, between the receiver and the sender via the visual physical channel, that the data is from the sender by having the receiver respond by sending a repeating nonce to the sender, wherein the repeating nonce is an action requested in the nonce.

2. (currently amended) The method according to claim 1, ~~wherein the data includes:~~

~~a key; and~~

~~a nonce~~

wherein the repeating nonce is a hand gesture.

3. (currently amended) ~~The method according to claim 2, wherein the verifying comprises one of:~~

~~performing receiver-initiated verification; and~~

~~performing sender-initiated verification.~~ The method according to claim 1, wherein the repeating nonce is an audio signal.

4. (currently amended) ~~The method according to claim 3, wherein~~

~~the performing receiver-initiated verification comprises:~~

~~repeating, by the receiver upon receiving the data, the nonce to generated a repeating nonce;~~

~~perceiving, by the sender, the repeating nonce;~~

~~verifying the perceived repeating nonce is semantically related to the nonce sent; and~~

~~acknowledging, to the receiver, that the receiver-initiated verification is successful, if the perceived repeating nonce is verified.~~

~~the performing sender-initiated verification comprises:~~

~~repeating, by the sender after the sending, the nonce sent to the receiver to generated a repeating nonce;~~

~~perceiving, by the receiver after receiving the data, the repeating nonce;~~

~~verifying the perceived repeating nonce is the same as the nonce received; andacknowledging, to the sender, that sender-initiated verification is successful, if the perceived repeating nonce is verified~~

The method according to claim 1, wherein after the sender verifies the repeating nonce, the sender sends a signed message.

5. (currently amended) The method according to claim [[2]] 4, further ~~comprising~~ including:

storing, by the receiver, the key received from the sender as a stored key, if the verifying is successful;

~~sending, from the sender to the receiver, if the verifying is successful, a signed~~

~~message;~~

receiving, at the receiver, the signed message; and

verifying [[the]] a signature in the signed message using the stored key.

6. (currently amended) A method for a sender, comprising:

establishing a physical channel with a receiver;

sending, from the sender to the receiver, data through a data channel, the data including a key and a nonce; and

verifying, between the sender and the receiver via the physical channel, that the receiver receives the data from the sender by receiving a repeating nonce from the receiver, the responding nonce being a response to an action requested by the nonce.

7. (currently amended) The method according to claim 6, wherein the ~~data includes:~~

~~a key; and~~

~~a nonce~~

repeating nonce is one of a sum of two numbers transmitted as the nonce; a multiplication of the two numbers, or a division of the two numbers.

8. (currently amended) ~~The method according to claim 7, wherein the verifying comprises one of:~~

~~performing receiver-initiated verification, comprising;~~

~~repeating, by the receiver upon receiving the data, the nonce received from the sender to generate a repeating nonce;~~

~~perceiving, by the sender, the repeating nonce;~~

~~verifying that the perceived repeating nonce is same as the nonce sent to~~

~~the receiver; and~~

~~acknowledging, to the receiver, that the receiver-initiated verification is successful, if the perceived repeating nonce is verified; and~~

~~performing sender-initiated verification, comprising:~~

~~repeating, by the sender after the sending, the nonce sent to the receiver to generate a repeating nonce;~~

~~perceiving, by the receiver upon receiving the data, the repeating nonce;~~

~~verifying that the repeating nonce is same as the nonce received; and~~

~~acknowledging, to the sender, that sender-initiated verification is successful, if the perceived repeating nonce is verified~~

The method according to claim 6, wherein the repeating nonce is an audio signal including a phrase spoken in a language requested in the nonce.

9. (currently amended) The method according to claim [[7]] 6, further ~~comprising~~ including sending, from the sender to the receiver, if the verifying is successful, a signed message.

10. (currently amended) A method for a receiver, comprising:

establishing a physical channel with a sender;

receiving, from the sender, data via a data channel, the data including a key and a nonce; and

verifying, between the sender and the receiver via the physical channel, that the data, received by the receiving, is from the sender by sending a repeating nonce, the repeating nonce including an action requested in the nonce.

11. (currently amended) The method according to claim 10, ~~wherein the data~~

~~includes:~~

~~a key; and~~

~~a nonce~~

wherein the repeating nonce is an audio signal including a phrase spoken in a language requested in the nonce.

12. The method according to claim ~~11, wherein the verifying comprises one of:~~

~~performing receiver-initiated verification, comprising:~~

~~repeating, by the receiver upon receiving the data, the nonce received from the sender to generate a repeating nonce;~~

~~perceiving, by the sender, the repeating nonce;~~

~~verifying that the perceived repeating nonce is same as the nonce sent to the receiver; and~~

~~acknowledging, to the receiver, that the receiver-initiated verification is successful, if the perceived nonce is verified; and~~

~~performing sender-initiated verification, comprising:~~

~~repeating, by the sender after the sending, the nonce to generate a repeating nonce;~~

~~perceiving, by the receiver upon receiving the data, the repeating nonce;~~

~~verifying that the perceived repeating nonce is same as the nonce received; and~~

~~acknowledging, to the sender, that sender-initiated verification is successful if the perceived repeating nonce is verified~~

10, wherein the repeating nonce includes a value corresponding to the addition of two numbers, the two numbers being included in the nonce.

13. (currently amended) The method according to claim [[11]] 10, further ~~comprising~~ including:

storing, by the receiver, the key received from the sender as a stored key, if the verifying is successful;

receiving, at the receiver, a signed message; and

verifying the signature in the signed message using the stored key.

14. (currently amended) A system, comprising:

a sender for sending data;

a data channel through which the sender sends data including a nonce and a key;

a receiver for receiving the data sent from the sender via the data channel; and

a visual physical channel, established between the sender and the receiver who are in visible range of each other, through which the receiver verifies that the data received by the receiver is from the sender, the receiver verifying by sending a repeating nonce, the repeating nonce including an action requested in the nonce.

15. (currently amended) The system according to claim 14, wherein the sender ~~comprises~~ includes:

an information generation mechanism for generating the data, the data including the key and the nonce; and

a transmitter for transmitting the data to the receiver via the data channel~~; and~~

~~a first verification mechanism for verifying, via the visible physical channel, that the data received by the receiver is from the sender~~.

16. (currently amended) The system according to claim [[15]] 14, wherein the receiver ~~comprises~~ includes:

a transmission receiver for intercepting the data, sent from the sender through the data channel; and

~~a second verification mechanism for verifying, via the physical channel and cooperating with the first verification mechanism in the sender, that the data received is from the sender; and~~

a key storage for storing [[a]] the key included in the received data, if the verifying is successful.

17. (currently amended) The system according to claim 16, wherein

the sender further ~~comprising~~ including a signed message generation mechanism for generating a signed message to be sent, after the verifying, to the receiver through the transmitter, the signed message including a signature of the sender; and

the receiver further comprising a signature verification mechanism for verifying, upon receiving the signed message, the signature of the sender received through the transmission receiver.

18. (currently amended) A system for a sender, comprising:

an information generation mechanism for generating data, the data including a key and a nonce;

a transmitter for transmitting the data to a receiver via a data channel; and

a verification mechanism for verifying, via a physical channel established between the sender and the receiver, that the data received by the receiver is from the sender by receiving a repeating nonce, the repeating nonce including a value of an action requested in the nonce.

19. (currently amended) The system according to claim 18, wherein the ~~verification mechanism includes one of:~~

~~a receiver-initiated verification mechanism for performing a receiver-initiated verification, comprising:~~

~~repeating, by the receiver upon receiving the data, the nonce received from the sender to generate a repeating nonce;~~

~~perceiving, by the sender, the repeating nonce;~~

~~verifying that the perceived repeating nonce is same as the nonce sent to the receiver; and~~

~~acknowledging, to the receiver, that the receiver-initiated verification is successful, if the perceived nonce is verified; and~~

~~a sender-initiated verification mechanism for performing a sender-initiated verification, comprising:~~

~~an nonce repeater for generating a repeating nonce using the nonce contained in the data sent to the receiver; and~~

~~an acknowledgement perceiver for perceiving an acknowledgement from the receiver that acknowledge that the repeating nonce is same as the nonce contained in the data~~

repeating nonce is a value of an addition of two numbers, the two numbers being originally sent in the nonce.

20. (currently amended) The system according to claim [[19]] 18, further ~~comprising~~ including a signed message generation mechanism for generating a signed message to be sent, after the verifying, to the receiver through the transmitter, the signed message including a signature of the sender.

21. (currently amended) A system for a receiver, comprising:

a transmission receiver for intercepting data, sent from a sender through a data channel, the data including a key and a nonce;

a verification mechanism for verifying, via a physical channel established between the sender and the receiver, that the data received is from the sender by sending a repeating nonce, the repeating nonce including an action requested in the nonce; and

a key storage for storing a key included in the received data, if the verifying is successful.

Claim 22 (cancelled).

23. (currently amended) The system according to claim [[22]] 21, further ~~comprising~~ including a signature verification mechanism for verifying the signature of the sender contained in a signed message, sent from the sender after the verifying and received by the receiver through the transmission receiver.

Claims 24 and 25 (cancelled).

26. (currently amended) A computer-readable medium encoded with a program ~~for a sender~~, the program including instructions, which when executed, ~~causing~~ cause a sender computer to:

send[[ing]], from a sender to a receiver, data through a data channel, the data including a key and a nonce;

send[[ing]], from the sender to the receiver a signed message, after verifying, ~~between the sender and the receiver~~ via a physical channel, that the data received by the receiver is from the sender by verifying that a repeating nonce received from the receiver includes an action requested in the nonce sent by the sender.

27. (currently amended) The medium according to claim 26, wherein ~~the verifying includes one of:~~

~~performing receiver-initiated verification via the physical channel; or~~

~~performing sender-initiated verification via the physical channel~~

the repeating nonce is a value of an addition of two numbers, the two numbers being sent in the nonce.

28. (currently amended) A computer-readable medium encoded with a program ~~for a receiver~~, the program including instructions, which when executed, ~~causing~~ cause a receiver computer to:

~~receiving~~ receive, from a sender, data via a data channel, the data including a key and a nonce;

transmit a repeating nonce to the sender, the repeating nonce including an action requested in the nonce;

~~storing~~ store ~~a part of the data~~ the key received from the sender ~~as a stored key~~, after verifying the repeating nonce is consistent with the nonce ~~verifying between the sender and the receiver via a physical channel, that the data received is from the sender~~;

~~receiving~~ receive, from the sender after the verifying, a signed message containing a signature of the sender; and

~~authenticating~~ authenticate the signature in the signed message using the stored key.

29. (currently amended) The medium according to claim 28, wherein ~~the verifying includes one of:~~

~~performing receiver-initiated verification via the physical channel; or~~

~~performing sender-initiated verification via the physical channel~~ the repeating nonce is a value of an addition of two numbers, the two numbers being included in the nonce.

30. (new) The medium according to claim 26, wherein the repeating nonce is an audio signal including a phrase spoken in a language as requested in the nonce.

31. (new) The medium according to claim 28, wherein the repeating nonce is an audio signal including a phrase spoken in a language as requested in the nonce.